UNITED STATES DISTRICT COURT

MIDDLE DISTRICT OF NORTH CAROLINA

TRACY GUIANG, individually and on behalf of all others similarly situated, and ALLISON BLANK, individually and on behalf of all others similarly situated, Plaintiffs, v. KRISPY KREME DOUGHNUT CORPORATION, Defendant.	Case No. 1:25-CV-499 **CLASS ACTION COMPLAINT** JURY DEMAND

COMES NOW Plaintiffs Tracy Guiang and Allison Blank ("Plaintiffs"), individually and on behalf of all others similarly situated, and on behalf of the general public, upon personal knowledge of facts pertaining to them and upon information and belief as to all other matters, and by and through undersigned counsel, hereby brings this Class Action Complaint against Defendant Krispy Kreme Doughnut Corporation ("Krispy Kreme" or "Defendant"), and alleges as follows:

I. INTRODUCTION

1. Plaintiffs bring this action on behalf of themselves, and all other individuals similarly situated ("Class Members") against Krispy Kreme for its failure to secure and safeguard the personally identifiable information ("PII") and private health information ("PHI") of Plaintiffs and Class Members.

2. Krispy Kreme is an American multinational doughnut and coffeehouse company incorporated in the State of North Carolina and maintains its corporate offices and principal place of business in Winston-salem, North Carolina. In the regular course of its business, Krispy Kreme

is required to maintain reasonable and adequate security measures to secure, protect, and safeguard their customers' and employees' PII/PHI against unauthorized access and disclosure.

3. On November 29, 2024, Krispy Kreme became aware that an unauthorized third party gained access to Krispy Kreme's information technology systems and accessed information containing PII/PHI of Krispy Kreme's customers and employees.

4. Krispy Kreme owed a duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Krispy Kreme breached that duty by, among other things, failing to, or contracting with companies that failed to, implement and maintain reasonable security procedures and practices to protect patients' PII/PHI from unauthorized access and disclosure. Every year, millions of Americans have their most valuable PII stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies still fail to make the necessary investments to implement important and adequate security measures to protect their customers' and employees' data.

5. Kripsy Kreme obtains its clients' and employees' sensitive PII/PHI and failed to protect it. Kripsy Kreme had an obligation to secure customers' and employees' PII/PHI by implementing reasonable and appropriate data security safeguards.

6. As a result of Krispy Kreme's failure to provide reasonable and adequate data security, Plaintiffs' and the Class Members' unencrypted, non-redacted PII/PHI has been exposed to unauthorized third parties. Plaintiffs and the Class are now at much higher risk of identity theft and cybercrimes of all kinds, especially considering the highly sensitive PII/PHI stolen here and the fact that the compromised PII/PHI is likely already being sold on the dark web. This risk constitutes a concrete injury suffered by Plaintiffs and the Class as they no longer have control over their

PII/PHI, which PII/PHI is now in the hands of third-party cybercriminals. This substantial and imminent risk of identity theft has been recognized by numerous courts as a concrete injury sufficient to establish standing.

7. Plaintiffs and the Class will have to incur costs to pay a third-party credit and identity theft monitoring service for the rest of their lives as a direct result of the Data Breach.

8. Plaintiffs bring this action on behalf of themselves and those similarly situated to seek redress for the lifetime of harm they will now face, including, but not limited to, reimbursement of losses associated with identity theft and fraud, out-of-pocket costs incurred to mitigate the risk of future harm, compensation for time and effort spent responding to the Data Breach, the costs of extending credit monitoring services and identity theft insurance, and injunctive relief requiring Krispy Kreme to ensure that it implements and maintains reasonable data security practices going forward.

II. THE PARTIES

9. Plaintiff Tracy Guiang is a resident of South Carolina, whose Personal Information was compromised in the Data Breach.

10. Plaintiff Allison Blank is a resident of California, whose Personal Information was compromised in the Data Breach.

11. Defendant Krispy Kreme is a North Carolina corporation, with its headquarters and principal place of business located at 370 Knollwood Street, Suite 500, Winston-salem, North Carolina 27103.

III. JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d) because there are more than 100 Class Members, at least one class member, including Plaintiffs, is a citizen of a state different from that of Krispy Kreme, and

the amount in controversy exceeds $5 million, exclusive of interest and costs.

13. This Court has personal jurisdiction over Krispy Kreme because it maintains its principal place of business in North Carolina.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Krispy Kreme's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiffs' and Class Members' claims occurred in this District.

IV. GENERAL ALLEGATIONS COMMON TO ALL COUNTS

15. This is a class action brought by Plaintiffs, individually and on behalf of all citizens who are similarly situated (i.e. the Class Members), seeking to redress Krispy Kreme's willful and reckless violations of their privacy rights. Plaintiffs and the other Class Members were customers/employees of Krispy Kreme.

16. On November 29, 2024, Krispy Kreme became aware that an unauthorized third party accessed Plaintiffs' and the Class Members' PII/PHI.

17. This action pertains to Krispy Kreme's unauthorized disclosures of the Plaintiffs' PII/PHI that occurred on November 29, 2024 (the "Breach").

18. Krispy Kreme disclosed Plaintiffs' and the other Class Members' PII/PHI to unauthorized persons as a direct and/or proximate result of Krispy Kreme's failure to safeguard and protect their PII/PHI.

19. By obtaining, collecting, and storing the PII/PHI of Plaintiffs and Class Members, Krispy Kreme assumed legal and equitable duties and knew or should have known it was responsible for protecting the PII/PHI from unauthorized disclosures.

20. Despite recognizing its duty to do so, Krispy Kreme failed to implement security safeguards to protect Plaintiffs' and the Class Members' PII/PHI.

21. Plaintiffs and Class Members have taken reasonable steps to maintain the

confidentiality of their PII/PHI and relied on companies, such as Krispy Kreme to keep their PII/PHI confidential and maintained securely, to use this information for business purposes only, to make only authorized disclosures of this information.

1. The Data Breach

22. According to a data breach notification ("Breach Notice") issued by Krispy Kreme on its website (https://www.krispykreme.com/notice-data-breach), Krispy Kreme discovered unauthorized access to its network systems on November 29, 2024. During this time, an unauthorized third party accessed files/information containing PII and PHI of customers and employees, including: name, Social Security number, date of birth, driver's license or state ID number, financial account information, financial account access information, credit or debit card information, credit or debit card information in combination with a security code, username and password to a financial account, passport number, digital signature, username and password, email address and password, biometric data, USCIS or Alien Registration Number, US military ID number, medical or health information, and health insurance information.

23. Kripsy Kreme first identified suspicious activity within its information technology systems on November 29, 2024, resulting in an alleged immediate investigation. On May 22, 2025, Krispy Kreme determined that certain personal information was affected.

24. The Breach Notice posted by Krispy Kreme did not specify detailed measures or actions taken by Krispy Kreme to fully remediate the vulnerabilities that led to the Data Breach, nor did it explain specific measures adopted to prevent future incidents.

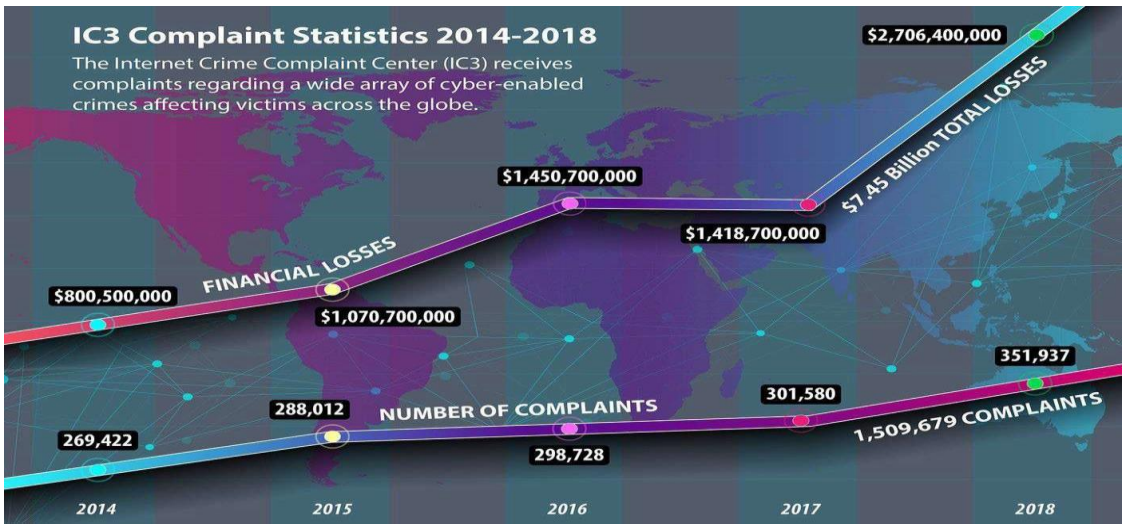
2. The Data Breach was Preventable

25. Had Krispy Kreme maintained industry-standard safeguards to monitor, assess, and update security controls and related system risks, Krispy Kreme could have safeguarded customer and employee data. Krispy Kreme's lack of security controls and implementation of enhanced

security measures only after the Data Breach are inexcusable.

26. Krispy Kreme was at all times fully aware of its obligation to protect customers' and employees' PII/PHI and the risks associated with failing to do so. Krispy Kreme knew that information of the type collected, maintained, and stored by Krispy Kreme is highly coveted and a frequent target of hackers.

27. This exposure, along with the fact that the compromised PII/PHI is already likely being sold on the dark web, is tremendously problematic. Cybercrime is rising at an alarming rate, as shown in the FBI's Internet Crime Complaint statistics chart shown below:



28. By 2013, it was being reported that nearly one out of four data breach notification recipients become a victim of identity fraud.[1]

29. Stolen PII is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

30. When malicious actors infiltrate companies and copy and exfiltrate the PII that those

[1] Pascual, Al, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," *Javelin* (Feb. 20, 2013).

companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[2]

31. In April 2023, NationsBenefits, "disclosed that thousands of its members had their personal information compromised in a late-January ransomware attached targeting Fortra's Anywhere platform, a file-transfer software that the firm was using. According to the news reports, the ransomeware gang CLOP claimed responsibility for the attack, saying it took advantage of a previously known vulnerability."[3]

32. In mid-April 2023, "the second largest health insurer [Point32Health], in Massachusetts, suffered major technical outages resulting from a ransomware attack. The incident brought down the company's systems that it uses to service members and providers, resulting in some members having difficulty contacting their insurers."[4]

33. In May 2023, MCNA Insurance Company disclosed that "personal health information of nearly nine million patients was compromised in a cyber incident discovered in March. In a data breach notification letter filed with the Maine state attorney general's office dated May 26, the firm said that it detected unauthorized access to its systems on March 6, with some found to be infected with malicious code…According to MCNA, the hackers were successful in accessing patient personal information."[5]

34. In April 2020, ZDNet reported in an article titled, "Ransomeware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomeware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage,

---

[2] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web- identity- monitoring (last accessed July 28, 2021).

[3] https://www.insurancebusinessmag.com/us/guides/the-insurance-industry-cyber-crime-report-recent-attacks-on-insurance-businesses-448429.aspx (Last visited August 22, 2023).

[4] *Id.*

[5] *Id.*

leak corporate information on dark web portals, and even tip journalists to generate negative news complaints as revenge against those who refuse to pay."[6]

35. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomeware Guide" advising that "[m]alicious actors have adjusted their ransomeware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[7]

36. Another example is when the U.S. Department of Justice announced its seizure of AlphaBay in 2017. AlphaBay had more than 350,000 listings, many of which concerned stolen and fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers, and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[8]

37. The PII of consumers remains of high value to criminals, as evidenced by the price they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and

---

[6] https://www.zdnet.com/article/ransomeware-mentioned-in-1000-sec-filings-over-the-past-year/ (Last visited August 22, 2023).

[7] https://www.cisa.gov/sites/default/files/2023-01-CISA_MS-ISAC_Ransomware%20Guide_8508C.pdf (Last visited August 22, 2023).

[8] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:*https://www.armor.com/resources/blog/s tolen-pii-ramifications- identity-theft-fraud-dark-web/ (Last visited July 28, 2021).

bank details have a price range of $50 to $200.[9] Experian reports that a solen credit or debit card number can sell for $5 to $110 on the dark web.[10] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[11]

38. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number assuming your identity can cause a lot of problems.[12]

39. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventative action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraudulent activity to obtain a new number.

40. Even then, a new Social Security number may not be effective. According to July Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the

---

[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal- data-sold- on-the-dark-web-how-much-it-costs/ (Last visited July 28, 2021).

[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask- experian/heres-how-much- your-personal-information-is-selling-for-on-the-dark-web/ (Last visited July 28, 2021).

[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the- dark/ (Last visited July 28, 2021).

[12] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (Last visited August 22, 2023).

new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

41. Because of this, the information comprised in the Data Breach here is significantly more harmful to lose than the loss of, for example, credit card information in a retailer payment card breach because victims can simply cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

42. The PII compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[14]

43. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

44. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

45. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

---

[13] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen- by-anthem-s-hackers-has-millionsworrying- about-identity-theft (last visited July 28, 2021).

[14] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells- for-10x-price-of-stolen-credit-card-numbers.html (last visited July 28, 2021).

46. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

47. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[15] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will fact, "substantial costs and inconveniences repairing damage to their credit records… [and their] good name."[16]

48. The exposure of Plaintiffs' and Class Members' PII to cybercriminals will continue to cause substantial risk of future harm, including identity theft, that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off this highly sensitive information.

3. Krispy Kreme Failed to Comply with the Federal Trade Commission

49. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[17]

---

[15] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao- 07-737.pdf (last visited July 28, 2021).

[16] *Id.*

[17] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain- language/pdf0205-startwithsecurity.pdf (last visited July 28, 2021).

50. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business,* which established guidelines for fundamental data security principals for business.[18] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted form the system; and have a response plan ready in the event of a breach.[19]

51. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[20]

52. Highlighting the importance of protecting against phishing and other types of data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

4. The Impact of Data Breach on Victims

---

[18] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 22, 2023).

[19] *Id.*

[20] Federal Trade Commission, *Start With Security*, *supra footnote 17*.

53. Krispy Kreme's failure to keep Plaintiffs' and Class Members' PII/PHI secure has severe ramifications. Given the highly sensitive nature of the PII/PHI stolen in the Data Breach, Social Security numbers, first and last names, dates of birth, and medical information, hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. As a result, Plaintiffs have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

54. The PII exposed in the Data Breach is highly-coveted and valuable on underground markets. Identity thieves can use the PII to: (a) commit insurance fraud; (b) obtain a fraudulent driver's license or ID card in the victim's name; (c) obtain fraudulent government benefits; (d) file a fraudulent tax return using the victim's information; (e) commit medical and healthcare-related fraud; (f) access financial and investment accounts and records; (g) engage in mortgage fraud; and/or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

55. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be victims of several cybercrimes stemming from a single data breach.

56. Given the confirmed exfiltration of patient PII/PHI from Krispy Kreme many victims of the Data Breach have likely already experienced significant harms as the result of the Data Breach, including, but not limited to, identity theft and fraud. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing financial and insurance statements, checking credit reports, and spending time and effort searching for unauthorized activity.

57. It is no wonder, then, that identity theft exacts a severe emotional toll on its victims. The 2021 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 84% reported anxiety;
- 76% felt violated;
- 32% experienced financial related identity problems;
- 83% reported being turned down for credit or loans;
- 32% reported problems with family members as a result of the breach;
- 10% reported feeling suicidal.[21]

58. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48% reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1 reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[22]

59. Annual monetary losses from identity theft are in the billions of dollars. According

---

[21] https://www.idtheftcenter.org/wpcontent/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (Last visited June 8, 2025).

[22] *Id.*

to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts…individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

60. The unauthorized disclosure of sensitive PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[23]

61. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intent to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

62. As a result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm

---

[23] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—that the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

for which they are entitled to damages, including, but not limited to, the following:

a. The unconsented disclosure of confidential information to a third party;

b. Unauthorized use of their PII/PHI without compensation;

c. Losing the value of the explicit and implicit promises of data security;

d. Losing the value of access to their PII/PHI permitted by Krispy Kreme without their permission;

e. Identity theft and fraud resulting from the theft of their PII/PHI;

f. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

g. Anxiety, emotional distress, and loss of privacy;

h. The present value of ongoing credit monitoring and identity theft protection services necessitated by the Data Breach;

i. Unauthorized charges and loss of use of and access to their accounts;

j. Lowered credit scores resulting from credit inquiries following fraudulent activities;

k. Costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

l. The continued, imminent, and certainly impending injury flowing from potential fraud and identity theft posed by their PII/PHI being in the possession of one or more unauthorized third parties.

63. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and

effort associated with seeking reimbursement. The Department of Justice's Bureau of Justice Statistics found that identity theft victims, "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[24]

64. Plaintiffs and Class Members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more to work with a provider that has better data security. Seventy percent of consumers would provide less personal information to organizations that suffered a data breach.[25]

65. Plaintiffs and Class Members have a direct interest in Krispy Kreme's promises and duties to protect PII/PHI, i.e., that Krispy Kreme would *not increase* their risk of identity theft and fraud. Because Krispy Kreme failed to live up to its promises and duties in this respect, Plaintiffs and Class Members seek the present value of ongoing identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by Krispy Kreme's wrongful conduct. Through this remedy, Plaintiffs seek to restore themselves and Class Members as close to the same position as they would have occupied but for Krispy Kreme's wrongful conduct, namely its failure to adequately protect Plaintiffs' and the Class Members' PII/PHI.

66. Plaintiffs and Class Members further seek to recover the value of the unauthorized access to their PII/PHI permitted through Krispy Kreme's wrongful conduct. This measure of

[24] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 14, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (Last visited August 22, 2023).

[25] https://web.archive.org/web20220205174527/https://www.fireeye.com/blog/executive-perspective/2016/05/beyong_the_bottomli.html (Last visited August 15, 2023).

damages is analogous to the remedies for the unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII is non-rivalrous—the unauthorized use by. Another does not diminish the rights- holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use of the value of the IP—i.e., a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a nonpracticing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because: (a) Plaintiffs and Class Members have a protectible property interest in their PII/PHI; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; (c) rental value is established with reference to market value, i.e., evidence regarding the value of similar transactions.

67. Plaintiffs and Class Members have an interest in ensuring their PII/PHI is secured and not subject to further theft because Krispy Kreme continues to hold their PII/PHI.

V. CLASS ACTION ALLEGATIONS

68. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and the following proposed nationwide class (herein "the Class"), defined as follows:

> **Nationwide Class**
> All persons residing in the United States whose personally identifiable information or personal health information was accessed by and disclosed in the Data Breach to unauthorized persons, including all who were sent a notice of the Data Breach.

69. Excluded from the proposed Class are any officer or director of Krispy Kreme; any officer or director of any affiliate, parent, or subsidiary of Krispy Kreme that transmitted the PII and PHI of the Nationwide Class; anyone employed by counsel in this action; and any judge to

whom this case is assigned, his or her spouse, and members of the judge's staff.

70. **Numerosity.** Members of the proposed Class are likely to number in the hundreds of thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Krispy Kreme's own records.

71. **Commonality and Predominance.** Common questions of law and fact exist as to the proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Krispy Kreme engaged in the wrongful conduct alleged herein;

b. Whether Krispy Kreme's inadequate data security measures was a cause of the Data Breach;

c. Whether Krispy Kreme owed a legal duty to Plaintiffs and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII and/or PHI;

d. Whether Krispy Kreme negligently or recklessly breached legal duties owed to Plaintiffs and the Class Members to exercise due care in collecting, storing, and safeguarding their PII and/or PHI;

e. Whether Plaintiffs and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Krispy Kreme failed to implement and maintain reasonable security procedures and practices for Plaintiffs' and Class Members' PII in violation of Section 5 of the FTC Act;

g. Whether Plaintiffs and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

72. Krispy Kreme engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, individually, and on behalf of the other Class Members. Similar or identical statutory and common violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous

questions that dominate this action.

73. **Typicality:** Plaintiffs' claims are typical of the claims of the Members of the Class. All Class Members were subject to the Data Breach and had their PII or PHI accessed by and/or disclosed to unauthorized third parties. Krispy Kreme's misconduct affected all Class Members in the same manner.

74. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

75. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Krispy Kreme, making it impracticable for Class Members to individually seek redress for Krispy Kreme's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE

76. Plaintiffs reallege paragraphs 1 through 75 as if fully set forth herein.

77. Plaintiffs bring this claim individually and on behalf of the Class.

78. Krispy Kreme owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PII/PHI from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiffs' and Class Members' PII/PHI in Krispy Kreme's possession was adequately secured and protected.

79. Krispy Kreme owed, and continues to owe, a duty to Plaintiffs and the other Class Members to safeguard and protect their PII/PHI.

80. Krispy Kreme breached its duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiffs' and the other Class Members' PII/PHI.

81. It was reasonably foreseeable that Krispy Kreme's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the other Class Members' PII/PHI would result in an unauthorized third-party gaining access to such information for no lawful purpose.

82. As a direct result of Krispy Kreme's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and the Class Members' confidential medical information, Plaintiffs and the Class Members suffered damages, including, without limitation, loss of the benefit of the bargain, exposure to heightened future risk of identity theft, increased infiltrations into their privacy through spam and/or attempted identity theft, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

83. By engaging in the negligent acts and omissions alleged herein, which permitted an unknown third party to access Krispy Kreme's systems containing the PII/PHI at issue, Krispy Kreme failed to meet the data security standards set forth under Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures, which Krispy Kreme has failed to do as discussed herein.

84. Krispy Kreme's failure to meet this standard of data security established under Section 5 of the FTC Act is evidence of negligence.

85. Neither Plaintiffs nor other Class Members contributed to the Data Breach as described in this Complaint.

86. Krispy Kreme's wrongful actions and/or inaction and the resulting Breach (as described above) constituted (and continue to constitute) negligence at common law.

87. As a result of Krispy Kreme's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Krispy Kreme's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
BREACH OF FIDUCIARY DUTY

88. Plaintiff realleges paragraphs 1 through 75 as if fully set forth herein.

89. Plaintiffs bring this claim individually and on behalf of the Class.

90. Plaintiffs and Class Members gave Krispy Kreme their PII/PHI in confidence, believing that Krispy Kreme would protect that information. Plaintiffs and Class Members would not have provided their PII/PHI had they known it would not be adequately protected. Krispy Kreme's acceptance, use, and storage of Plaintiffs' and Class Members' PII/PHI created a fiduciary relationship between Krispy Kreme

and Plaintiffs and Class Members. In light of this relationship, Krispy Kreme must act primarily for the benefit of Plaintiffs and the Class Members, which includes safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

91. Krispy Kreme has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. It breached that duty by, among other things, failing to, or contracting with third parties that failed to, properly protect the integrity of the system containing Plaintiffs' and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Class Members' PII/PHI that it collected, utilized, and maintained.

92. As a direct and proximate result of Krispy Kreme's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Krispy Kreme's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Petition, respectfully request that the Court enter judgment in their favor and against Krispy Kreme, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiffs as Class Representatives and appointing

Plaintiffs' counsel as Lead Counsel for the Class;

B. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seeks appropriate injunctive relief designed to prevent Krispy Kreme from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and the Class such other favorable relief as allowable under law.

Dated: June 20, 2025

Respectfully submitted,

/s/ Scott C. Harris

Scott C. Harris (Bar No. 35328)
Milberg Coleman Bryson Phillips Grossman LLC
900 W. Morgan Street
Raleigh, NC 27603
Telephone: (919) 600-5000
Email: sharris@milberg.com

Attorneys for Plaintiff